Inter-agency Advisory Board (IAB) Meeting Minutes

Date	Time	Location
May 13, 2005	9:30 AM - 12:00 PM	U.S. Department of Energy, Forrestal Building 1000 Independence Ave SW Washington, DC 20585

Discussion Topic 1: Opening Remarks	
Issue:	Opening Remarks/Administrative Items
Discussion/ Resolution/ Action Items	▪ Mr. Tony Cieri, on behalf of the Department of Homeland Security (DHS), introduced the new IAB chairperson, Mr. Mike Butler, Director, DoD Access Card Office (ACO). Mr. Butler will be co-chairing the IAB for the next several months with the former chairperson, Mr. Bob Donnelson, Department of Interior (DOI). ▪ Ms. Lynne Prince, Defense Manpower Data Center (DMDC), was recognized for her recent promotion to Access and Authentication Technology Division Chief within the DMDC. ▪ The IAB chairperson noted that the IAB does not have approval authority. The role of the IAB is to provide common information to all agencies that facilitates the sharing of information, applications, and development of solutions to promote interoperability and share/save costs on common needs. The IAB is chartered through the Federal Advisory Committee Act (FACA), and FACA's purpose is to ensure that advice given to the Executive Branch, by the various advisory committees, task forces, boards, and commissions formed over the years by Congress and the President, be both objective and accessible to the public.

Discussion Topic 2: The First Responder Project	
Issue:	Using Public Key Infrastructure (PKI) for physical security authorization.
Discussion/ Resolution/ Action Items	▪ The Director of Office of National Capital Region (NCR), Mr. Tom Lockwood, took on credentialing, in the form of the First Responder Project, for the NCR. The First Responders Passport project is a major initiative for DHS. The purpose is to provide a common identification credential that can be used for access across multi-jurisdictions (Federal, state, local, and private sector). This will allow personnel to rapidly gain access in and out of incident areas through the use of a trusted and secure credential. ▪ On February 25, 2005, the Federal Information Processing Standard (FIPS) 201 was approved by the Secretary of Commerce. The NCR First Responder project meets the requirements outlined in FIPS 201 and, as a result, the standard has provided a baseline for personal identity authentication and verification (PIV) of all First Responders and Emergency Support Function (ESF) personnel within, and outside, the Federal government throughout the U.S. ▪ By year end 2007, all appropriate individuals will be issued a First Responder Passport within Federal Emergency Management Agency (FEMA) Region III (including six states and communities). The number of states participating in the First Responder Passport initiative is consistently increasing. In addition, the Office of the NCR Coordination is obtaining PDA requirements and coordinating them with DoD and other user communities to promote a family of interoperable devices. DHS provided a demonstration of the First Responder handheld and the use of the chip technology being applied by DHS. ▪ For organizations looking forward to physical access control pilots, grant money will be available in the near-term for pilots and project; however, in order to be reimbursed for expenses, participating groups must use FIPS-201 certified technology. DoD and DHS will leverage the current technologies available and share lessons learned as they continue to work together to further enhance identity protection and management initiatives.

Discussion Topic 3: Development Status for a Common Handheld Device	
Issue:	Need common handheld requirements
Discussion/ Resolution/ Action Items	▪ As explained above, both DHS and DoD have developed physical access control systems that make use of handheld devices. The DHS handheld uses chip technology; meanwhile, DoD implemented a physical access control system, also known as the Defense Biometric Identification System (DBIDS), which uses barcode technology. Due to the differing technology, the handhelds are not interoperable with the credentials from the other program. In addition, there are other physical access programs that use handheld devices and different technology. There is a need for convergence of effort to promote interoperability, and a standard/specification to govern common identity 'appliances'. ▪ A small team within DoD conducted market research in the handheld vendor community. Before pressing forward with the development of a specification, additional input from Federal law enforcement personnel and industry representatives is required. The intent is to gain information on handheld requirements from a diverse cross-section of stakeholders in order to obtain a balance of firm requirements. If firm requirements are obtained, there are funds available for research and development. The objective is to develop a single standard and support a family of appliances, which will facilitate interoperability efforts. To accomplish this, consensus on cards, data formats, and transmission mediums for appliances is required. ▪ A joint DoD/DHS briefing is scheduled at an FBI event the week of 16 May 2005. The goal of this effort is to acquire devices for identity authentication that are developed to the FIPS-201/PIV standard and can be used by military and civilian law enforcement officials.

Discussion Topic 4: Placement of the Laser Etching as now Mandated by FIPS 201	
Issue:	Laser etching on back of card is moved in the new FIPS 201 standard.
Discussion/ Resolution/ Action Items	▪ At the start of the CAC program in 1999, DoD had the card number etched on the card, by laser, as opposed to printing it on the card. DoD made the laser etching a requirement in the DoD smart card pre-issuance specification, which resulted in card vendors applying investment funds to comply with the specification. Since that time, all Federal agency smart card programs have applied the laser etching requirement as outlined in the DoD specification. ▪ FIPS-201 requires the card number to be etched by laser; however, the standard has relocated the number to a different area on the card than specified by the DoD specification. This change would be costly for the smart card vendors since they would have to retool their laser etching machines. Also, DoD would be required to change its pre-issuance specification. Instead, DoD proposes a change to the FIPS 201 standard that would allow the card number to be laser etched in the same position as it is currently outlined in the DoD smart card pre-issuance specification.

Discussion Topic 5: Logical Access	
Issue:	The logical access requirements outlined in the current FIPS-201 do not meet the definition of logical access requirements as defined by the IAB.
Discussion/ Resolution/ Action Items	▪ The FIPS-201 defines logical access purely as authentication to the network or logical system. Meanwhile, the IAB defines logical access more completely to mean authentication, encryption, and signing. According to the IAB, logical access should mean that once a user is authenticated they should be able to work (i.e. encrypt and sign e-mail). However, the FIPS-201 Standard does not explicitly define these additional capabilities, and in fact, it leaves these other key pairs (i.e. encrypting and signing keys) as optional. ▪ The IAB would like to move towards interoperability and mandatory keys for digital signature, encryption, and authentication. This is a difficult decision because it will require an increase in cost.

	▪ There is a need to assemble a team with logical access expertise to review the current FIPS logical access requirements, and develop a common set of implementation recommendations to propose to NIST.

Discussion Topic 6: Physical Access	
Discussion Points:	Physical access initiatives and lessons learned.
Discussion/ Resolution/ Action Items	▪ There are many disparate physical access initiatives going on in DoD; however, DoD is starting to see some convergence of efforts. As of May 2005, Ft. Hood, an Army base in Texas, has a physical access system that uses the CAC, DBIDS, RFID, and toll gates for entry onto its premises. The Ft. Hood implementation was a massive and successful integration effort, and it may be an example for future DoD implementations. In fact, a similar physical access pilot is taking place in the NCR at several DoD sites. ▪ DoD stood-up a lab at the Joint Interoperability Test Command (JITC) to identify a qualified vendor list for smart card technology. DoD also funded JITC to test contactless readers in order to decide on the best technology based on cost and security. Contactless technology is important for physical access to enable better throughput and ease of use. There is a JITC testing plan, funded by DoD, that will be posted on the website. ▪ NASA has a FIPS certified enterprise-wide physical access control system at all of NASA's facilities. NASA reports that the technology aspects of a physical access control system are easy compared to the policy and process issues that have to be worked out. ▪ DOI started their physical access control system effort in 2000 using MI-Fare technology. Currently, all DOI employees are using contactless technology to access facilities. Will continue to share lessons learned.

Discussion Topic 7: Pre-enrollment Isues	
Issue:	Make recommendations on how to deal with the FIPS-201 NACI requirements.
Discussion/ Resolution/ Action Items	▪ There are multiple issues involved with foreign national identity vetting. In particular, it is necessary to identify processes and procedures for performing an acceptable National Agency Check (NAC) equivalence for foreigners in order to make recommendations to NIST. ▪ It was noted that GSA has a task force working this particular issue. The discussion on foreign national clearance and suitability for credentials was tabled and awaiting further guidance from the GSA task force.

Discussion Topic 8: Training Modules	
Issue:	DoD and DOI would like to make a DoD-developed FIPS training module available for multiple agencies to use.
Discussion/ Resolution/ Action Items	▪ There are initial electronic training videos that DOI developed for their smart card implementation that can be made available for reference. ▪ Likewise, DoD recently contracted the development of a learning management system (LMS). The plan is to develop training modules that are Federal/FIPS 201 centered (i.e. not agency specific). Before these resources can be released, it is necessary to have them reviewed by the membership. ▪ IAB chairperson requested the membership review FIPS 201 DOI and LMS training modules for feedback.

Discussion Topic 09: Document Repository	
Issue:	Coordination efforts with Federal, State, and Local parties of interest as well as interested industry partners.
Discussion/ Resolution/ Action Items	▪ DoD started its smart card implementation five years ago, and has worked through a host of technical and policy issues. As a result, DoD will provide its program documentation, generalized, for mass consumption. The work involved with HSPD-12 is a labor intensive, but very noble, effort.

	▪ The ACO developed a document repository to share with Federal partners as well as the State and Local governments that are joining the HSPD credentialing effort. To access the website, privileges must be assigned and granted to proceed behind the DoD firewall. The plan is that this information will eventually be transferred and hosted by GSA.

Discussion Topic 10: Closing Remarks	
Issue:	
Discussion/ Resolution/ Action Items	▪ The IAB is requires energetic volunteers who will provide their expertise to define technical and business rules for the FIPS 201 implementation issues outlined above. The IAB intends to assemble a small task force to provide recommendations on some of the issues detailed above. Consensus recommendations developed by the task forces will be brought forward for consideration to the Office of Management and Budget (OMB) and the General Services Administration (GSA). ▪ The ACO posted its lessons learned and generalized specifications on its website in the 'Federal State and Local Interest' area. In order to access the 'Federal State and Local Interest' area of the ACO site, it is necessary to be registered with the ACO website. For access, please provide the following information to cacsupport@osd.pentagon.mil, and an account will be created for you. o First name o Last name o Agency/Org. o E-mail o Primary phone number ▪ Please note, if you are not accessing the ACO website from a .mil or a .gov domain, an additional step is required to grant you access through the DoD firewall. Since personal information is required in order to grant access, we request that you contact cacsupport@osd.pentagon.mil in order to complete the process. ▪ Details on the next meeting will be forthcoming.